AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

An Apple iPhone 7 Plus, with IMEI number: 353807084250860, Phone number: (937) 829-1012

Case No. 3:20MJ137

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to Commit Health Care Fraud and Wire Fraud
18 U.S.C. § 1347	Health Care Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Michael G. Pemberton
Applicant's signature

Michael Pemberton, Special Agent
Printed name and title

Sworn to before me and signed in my presence via facetime.

Date: 03/14/20

Judge's signature

City and state: DAYTON, OHIO

Hon. Sharon L. Ovington, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF: THE SEARCH OF An Apple iPhone 7 Plus, with IMEI number: 353807084250860, Phone number: (937) 829-1012	Case No. 3:20MJ137 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michael Pemberton, Special Agent for the Department of Health and Human Services, Office of the Inspector General, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Health and Human Services ("HHS"), Office of Inspector General ("OIG"), assigned to the Detroit, Michigan, Field Office. I joined the United States Air Force in 1995 and served nearly 13 years on active duty. In 2000, I graduated from the Air Force Office of Special Investigations ("AFOSI") Academy at Andrews Air Force Base, Maryland. I was an AFOSI Special Agent for the last seven years of my Air Force career. From August 2008 to June 2015, I was a Special Agent with the United States Environmental Protection Agency ("EPA"). Upon becoming an EPA Special Agent, I graduated from the Criminal Investigator Training Program at the

Federal Law Enforcement Training Center at Glynco, Georgia.

2. I have been a Special Agent with HHS-OIG since June 2015. As a Special Agent with HHS-OIG, I am responsible for investigating violations of United States federal law, including, but not limited to, Title 18, United States Code, Section 1347 (Health Care Fraud), Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1349 (Conspiracy to Commit Health Care Fraud and Wire Fraud), Title 18, United States Code, Section 371 (Conspiracy to Pay and Receive Illegal Remunerations), Title 42, United States Code, Section 1320a-7b(b) (Paying and Receiving Remunerations), Title 18, United States Code, Section 1035 (False Statements In A Health Care Matter), and 21 United States Code, Section 841 (Unlawful Distribution of a Controlled Substance). In connection with investigating these offenses, I have participated in the execution of search warrants for documents and other evidence in cases involving violations of these offenses, including at medical facilities, such as pharmacies, and individuals' residences.

PURPOSE OF THE AFFIDAVIT

3. I make this affidavit in support of an application to search a cellular telephone, with phone number (937) 829-1012, and IMEI number: 353807084250860 ("Subject Telephone"), or any phone assigned that phone number in the event that the number was previously assigned or re-assigned to a

different phone. Based upon information obtained by the Federal Bureau of Investigation ("FBI") and the Department of Health and Human Services ("HHS"), Office of the Inspector General ("OIG"), there is probable cause to believe, and I do believe, that Kindy Ghussin ("Ghussin") has billed Medicare, Medicaid, and other insurance for prescription medication that was not dispensed to patients.

4. The Subject Telephone to be searched is more fully described in the following paragraphs and in Attachment A. In Attachment B, I more fully describe the particular content of the Subject Telephone to be seized.

5. As discussed herein, the statements in this affidavit are based upon information obtained through the investigation in which I participated of Ghussin and others involved in a health care fraud scheme involving pharmacies in Michigan and Ohio. Since this affidavit is being submitted for the limited purpose of supporting a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause to believe evidence of crime, fruits of crime, contraband, and other items illegally possessed in violation of the aforementioned federal laws are located on the Subject Telephone.

6. Based on my training and experience, and the information set forth below, there is probable cause to believe that certain evidence and fruits and instrumentalities supporting violations of the following federal criminal statutes is

presently being maintained or stored on the Subject Telephone:

A. Title 18, United States Code, Section 1347, Health Care Fraud;

B. Title 18, United States Code, Section 1343, Wire Fraud;

C. Title 18, United States Code, Section 1349, Conspiracy to Commit Health Care Fraud and Wire Fraud; and

D. Title 21, United States Code, Section 841, Unlawful Distribution of a Controlled Substance.

VIOLATION STATUTES

7. Title 18, United States Code, Section 1347, prohibits health care fraud: Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice—

(1) to defraud any health care benefit program; or

(2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program,

in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 10 years, or both.

8. Title 18, United States Code, Section 1343, prohibits wire fraud: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses,

representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

9. Title 18, United States Code, Section 1349, provides that any person who attempts or conspires to commit health care fraud or wire fraud shall be subject to the same penalties as those set forth in 18 U.S.C. §§ 1347 and 1343.

10. Title 18, United States Code, Section 24(b), defines a "health care benefit program" as, among other things, "any public or private plan . . . affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service, for which payment may be made under the plan.

11. Title 21, United States Code, Section 841(a)(1), provides that it is unlawful for any person to knowingly or intentionally manufacture, distribute, dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance.

THE MEDICARE AND MEDICAID PROGRAMS

12. The Medicare Program ("Medicare") is a federally funded health care program providing benefits to persons who are sixty-five years of age or older or disabled. Medicare is administered by the Centers for Medicare and Medicaid Services ("CMS"), a federal agency within the Department of Health and Human

Services ("HHS"). Individuals who receive Medicare benefits are Medicare "beneficiaries."

13. Medicare is a "health care benefit program," as defined by 18 U.S.C. § 24(b).

14. Medicare has four parts: hospital insurance (Part A), medical insurance (Part B), Medicare Advantage (Part C), and prescription drug benefits (Part D). Medicare Part B helps pay the cost of physician services, medical equipment and supplies, and other health services and supplies not paid by Part A. This investigation involves Medicare Part D, prescription drug benefits.

15. A pharmacy can participate in Medicare Part D by entering into a retail network agreement directly with a plan or with one or more Pharmacy Benefit Managers ("PBMs"). A PBM acts on behalf of one or more Medicare drug plans. Through a plan's PBM, a pharmacy can join the plan's network. When a Medicare Part D beneficiary presents a prescription to a pharmacy, the pharmacy submits a claim either directly to the plan or to a PBM that represents the beneficiary's Medicare drug plan. The plan or PBM determines whether the pharmacy is entitled to payment for each claim and periodically pays the pharmacy for outstanding claims. The drug plan's sponsor reimburses the PBM for its payments to the pharmacy. PBMs sometimes contract with Pharmacy Services Administrative Organizations ("PSAOs") to administer some of its services, such as payments.

16. CVS Caremark, OptumRx, and Express Scripts are three of several PBMs.

CVS Caremark processes and adjudicates claims electronically in Arizona. OptumRx and Express Scripts process and adjudicate claims electronically outside the state of Michigan.

17. Medicare, through CMS, compensates the Medicare drug plan sponsors and pays the sponsors a monthly fee for each Medicare beneficiary of the sponsors' plans. Such payments are called capitation fees. The capitation fee is adjusted periodically based on various factors, including the beneficiary's medical conditions. In addition, in some cases where a sponsor's expenses for a beneficiary's prescription drugs exceed that beneficiary's capitation fee, Medicare reimburses the sponsor for a portion of those additional expenses.

18. By becoming a participating provider in Medicare, enrolled providers agree to abide by the policies, procedures, rules, and regulations governing reimbursement. To receive Medicare funds, enrolled providers, together with their authorized agents, employees, and contractors, are required to abide by all the provisions of the Social Security Act, the regulations promulgated under the Act, and applicable policies, procedures, rules, and regulations, issued by CMS and its authorized agents and contractors.

19. Medicare providers are required to maintain all records that disclose the extent of services provided and significant business transactions for a period of at least six years.

20. Qlarant is the Medicare Part C and Part D program integrity contractor for CMS under the National Benefit Integrity Medicare Drug Integrity Contract ("MEDIC"). Qlarant's role is to detect, prevent, and investigate allegations of fraud, waste, and abuse in the Part C (Medicare Advantage organizations) and Part D (prescription drug coverage) programs on a national level.

21. The Ohio Medicaid Program ("Medicaid") is a federal and state funded health care program providing benefits to individuals and families who meet specified financial and other eligibility requirements and certain other individuals who lack adequate resources to pay for medical care. CMS is responsible for overseeing the Medicaid program in participating states, including Ohio. Individuals who receive benefits under the Medicaid program are also referred to as "beneficiaries."

22. Medicaid covers the costs of medical services and products ranging from routine preventive medical care for children to institutional care for the elderly and disabled. Among the specific medical services and products provided by Medicaid are reimbursements to pharmacies for the provision of prescription drugs. Generally, Medicaid covers these costs if, among other requirements, they are medically necessary and ordered by a physician.

SUBJECT PHARMACIES

Heartland Pharmacy

23. Heartland Pharmacy LLC ("Heartland") was a registered business entity with

the Ohio Secretary of State. The following information is based on publicly available documents filed with the Ohio Secretary of State on Heartland's behalf. Heartland's Articles of Organization were filed on March 21, 2012 and reflect that Ghussin established the entity. Heartland's registered address was 3415 Riva Court, Beavercreek, Ohio 45430, which according to public records, including Ghussin's driver's license, is Ghussin's residence. Heartland's articles of organization list Ghussin as the statutory agent.

24. An FBI agent and I reviewed September 2014, December 2016, and December 2017 Express Scripts provider certifications for Heartland, all signed by Ghussin, which listed the practice address for the pharmacy as 3000 Far Hills Avenue, Kettering, Ohio, 45429. According to that documentation, Heartland had been open since at least the end of 2012. The September 2014 and December 2016 provider certifications reflect that Ghussin, Abeer Rizek, Hassan Abdallah ("Abdallah"), and Raef Hamaed ("Hamaed") each owned 25% of Heartland. The December 2017 provider certification lists Ghussin as a 34% owner, Abdallah as a 33% owner, and Hamaed as a 33% owner. All of the forms identify Ghussin as the pharmacist in charge ("PIC").

Heartland Pharmacy 2

25. Heartland Pharmacy 2, LLC ("Heartland 2") was a registered business entity with the Ohio Secretary of State. The following information is based on publicly

available documents filed with Ohio Secretary of State on Heartland 2's behalf. Heartland's Articles of Organization were filed on June 7, 2012 and reflect that Ghussin established the entity. Heartland 2's registered address was 3415 Riva Court, Beavercreek, Ohio 45430, which, as stated above, is Ghussin's residence. Heartland 2's articles of organization list Ghussin as the statutory agent.

26. An FBI agent and I reviewed a September 2014 Express Scripts provider certification for Heartland 2, which listed the practice address for the pharmacy as 2749 West Alex Bell Road, Moraine, Ohio 45459. According to that documentation, Heartland 2 had been open since at least approximately September 2012 and Ghussin, Abdallah, and Hamaed were each listed as owners. Ghussin was listed as a 33.34% owner, Abdallah was listed as a 33.33% owner, and Hamaed was listed as a 33.33% owner. Balhar Singh ("Singh") was listed as the PIC.

3415 Riva Court, Beavercreek, Ohio 45430

27. According to Ohio Secretary of State driver's license records, Ghussin's current address is listed as 3415 Riva Court, Beavercreek, Ohio 45430. A public records database search indicated that Ghussin's current address is 3415 Riva Court, Beavercreek, Ohio 45430.

FRAUD SCHEME

28. A common pharmacy fraud scheme is to bill Medicare, Medicaid, and other health insurers for medication that the pharmacy does not actually dispense to

patients. Put another way, at a high-level, the pharmacy is submitting a higher volume of medication in claims to Medicare, Medicaid, and other insurers than it purchased during the relevant period; based on my experience and training, this is often referred to as a "shortage" scheme. This is indicative of fraud because a pharmacy cannot dispense more medications than it has purchased. Typically, although not always, Medicare and Medicaid pay significant sums for these "shortage" medications. For example, inhalers and pain creams are common shortage medications because insurers may pay hundreds of dollars for those medications. However, pharmacies can bill but not dispense any medication. Over the course of the last four-plus years I have investigated shortage schemes, I have interviewed many patients, who have told me that both expensive and inexpensive medications (ranging from inhalers like Advair, Symbicort, QVAR, Spiriva, and HIV medication to creams and other items) were billed to Medicare, Medicaid, and other insurers that they never received from a particular pharmacy.

29. I will provide a simplified overview of how the shortage analysis is conducted to assist the Court in evaluating this search warrant application. In general, investigating a shortage scheme involves three steps: first, agents obtain a pharmacy's drug purchase records from pharmaceutical wholesalers. Agents identify wholesalers based on financial records for the pharmacy and its owner, which identify purchases from wholesalers, and submissions from the pharmacy to state

regulators and PBMs about the wholesalers used by the pharmacies; second, agents obtain Medicare and Medicaid claims data for the pharmacy; third, agents request that Qlarant conduct a shortage analysis for the time period for which it has drug purchase records and claims data.

30. Using the pharmacy's purchase records from the wholesalers and the claims data, Qlarant will pick a representative sample of prescription medications and compare the volume purchased with the volume dispensed in Medicare and Medicaid claims. Qlarant will then identify the volume of any shortage for each medication reviewed and the estimated amount that Medicare and Medicaid would have paid for medication billed but not dispensed. Because this analysis generally does not include claims data from any private insurers, the shortage amounts are conservative numbers because they do not incorporate any claims for that medication billed to private insurers.

31. Based on the shortage analyses performed in this investigation, the owners and operators of the aforementioned pharmacies fraudulently billed Medicare, Medicaid, and other insurers for medications that were not dispensed to beneficiaries. The pharmacies did not have sufficient drug inventory to dispense numerous expensive medications billed to Medicare and Medicaid.

32. Pharmacies will also submit claims for medications disbursed to patients that post-date the date the patient died. Often, this is because the pharmacy has an

automatic refill system in place that sends a claim to Medicare, Medicaid, and other insurers after a certain time period has passed since the prior fill of that prescription. However, whether a prescription is an automatic refill or not, if a patient does not pick up a prescription, the pharmacy is obligated to reverse the claim within a certain time. In my training and experience, pharmacies committing fraud often submit claims for beneficiaries who are already dead and never reverse them. The pharmacies involved in this investigation submitted post-death claims.

33. The owners/operators of the aforementioned pharmacies submitted false and fraudulent claims through interstate wires from Ohio to Medicare and Medicaid. The claims were processed and adjudicated electronically by CVS Caremark, OptumRx, and Express Scripts, among other PBMs, outside the state of Ohio.

PROBABLE CAUSE FOR SUBJECT TELEPHONE

Cooperating Witnesses

34. Cooperating Witness 1 ("CW-1") is known to agents, including me. CW-1 pleaded guilty to conspiracy to commit health care fraud in the Eastern District of Michigan. CW-1 has not yet been sentenced. CW-1 owned a pharmacy and pleaded guilty stemming from a scheme in which CW-1's pharmacy billed for prescriptions that were not dispensed and paid kickbacks to induce beneficiaries to fill their prescriptions at CW-1's pharmacy. FBI and HHS-OIG agents in Michigan, including me, interviewed CW-1 in March 2017 and February 2020. CW-1 provided the

following information based on conversations CW-1 had with Abdallah.

35. CW-1 knows Abdallah. They had multiple conversations, including some as recently as 2016, about their respective pharmacies and the fraud schemes they were each engaged in. Abdallah told CW-1 that Abdallah owned a pharmacy in Ohio that he had sold and another pharmacy that he opened in Ohio. FBI and HHS-OIG agents in Michigan, including me, reviewed records in this case indicating that Abdallah sold his interest in a pharmacy in Ohio in approximately 2012 or 2013 and subsequently opened Heartland and Heartland 2 with Ghussin and Hamaed.

36. Abdallah told CW-1 that Abdallah partnered with different individuals for his pharmacies, including Hamaed. Abdallah told CW-1 that Abdallah submitted claims for prescriptions that he did not dispense and submitted claims for automatic refills even if the patient did not want the medication. Abdallah stated that if his pharmacies were audited, he would be in trouble. Abdallah stated that he tried to conceal his shortages by keeping enough inventory and invoices to cover an invoice review by the PBM for which the pharmacy billed through the most.

37. Cooperating Witness 2 ("CW-2"), a relative of CW-1, is known to agents and pleaded guilty to conspiracy to commit health care fraud in the Eastern District of Michigan. CW-2 has not yet been sentenced. CW-2 owned a pharmacy and worked at a different pharmacy and pleaded guilty stemming from a scheme in which these pharmacies billed for prescriptions that were not dispensed and paid kickbacks to

induce beneficiaries to fill their prescriptions these pharmacies. FBI and HHS-OIG agents in Michigan, including me, interviewed CW-2 in March 2017 and February 2020 and CW-2 provided the following information based on conversations CW-2 had with Abdallah.

38. CW-2 knows Abdallah. They had multiple conversations between 2010 and 2014 about their respective pharmacies and the fraud schemes they were each engaged in. Abdallah told CW-2 that Abdallah partnered with different individuals for his pharmacies, including Hamaed. Abdallah told CW-2 that Abdallah submitted claims for prescriptions that he did not dispense and submitted claims for automatic refills even if the patient did not want the medication without reversing the claims. Abdallah stated that if his pharmacies were audited, he would be in trouble. Abdallah stated that he tried to conceal his shortages by keeping enough inventory and invoices to cover an invoice review by the largest PBM. He told his partners to do this as well. Abdallah also stated that he closed and opened pharmacies on multiple occasions to avoid detection.

Heartland

Qlarant Invoice Reconciliation

39. An FBI agent and I requested drug purchase records and received responses from the pharmaceutical wholesalers used by Heartland, which are listed below. An FBI agent and I furnished all of the wholesaler records and Medicare and Medicaid

data received to Qlarant and requested an invoice review for the period of December 4, 2012 through June 4, 2019. Qlarant compared invoices for Heartland's drug purchases to Medicare and Medicaid claims data for this period.

40. On November 22, 2019, Qlarant provided the following summary of its invoice review:

> **Wholesalers with Supportive Invoices:** Akron, Alpine, Anda, Auburn, Bonita, Cardinal, DTR Medical, Fagron, H&H Wholesaler, Health Source, Independent, Ixthus, Letco Medical, Masters, McKesson, Medmax, Miami Luken, Nephron, NuMed, Paragon, ParMed, Pharmsource, Praxis, Prescription Supply, PriMed, Redmond & Greer, Republic, River City, Smith Drug and Integral, South Pointe, Taiga, and Wasatch
>
> **Date Range of Invoice Review:** 12/04/2012 – 6/04/2019
>
> **Number of Drugs Reviewed:** 179
>
> **Total Number of Drugs Short to Medicare:** 55
>
> **Total Number of Drugs Short to Medicaid:** 4
>
> **Approximate Loss to Medicare:** $661,857.23
>
> **Approximate Loss to Medicaid:** $28,731.69
>
> **Approximate Combined Loss to Medicare and Medicaid:** $690,588.92

41. Qlarant provided the following summary of Heartland's top ten drug shortages by approximate combined loss to Medicare and Medicaid:

Drug Name	Approx. Dollar Loss
Novolog Inj Flexpen	$97,403.51
Metformin Tab 1000 ER	$66,818.75
Lantus Solos Inj 100/ML	$58,232.55
Seroquel XR Tab 300 MG	$45,834.94

Drug Name	Approx. Dollar Loss
Abilify Tab 10 MG	$45,275.24
Budesonide Cap 3 MG DR	$29,617.53
Abilify Tab 20 MG	$27,561.16
Creon Cap 24000 UNT	$25,464.72
Renvela Pow 2.4 GM	$24,067.49
Humulin R Inj U-500	$23,120.56

42. In sum, Qlarant concluded that Heartland's inventory of prescription drugs was not sufficient to support its claim submissions to Medicare and Medicaid for at least 55 of the 179 drugs selected for the analysis. Based upon the shortage detected, Qlarant concluded that Medicare and Medicaid paid Heartland approximately $690,588.92 for medications that Heartland did not have sufficient inventory to dispense. The shortage drugs that caused the highest dollar loss were Novolog Inj Flexpen, Metformin Tab 1000 ER, and Lantus Solos Inj 100/ML.

Beneficiary Interview

43. In December 2019, An FBI agent and I interviewed S.H., a Medicare beneficiary who picked up prescriptions at Heartland. Claims data reflects prescriptions purportedly dispensed to S.H. from at least 2013 to 2018. S.H. identified Ghussin as the pharmacist and owner of Heartland. S.H. stated that s/he did not receive all of the medication that Heartland billed to his/her Medicare insurance.

44. For example, S.H. only received Metformin Tab 500 mg ER from Heartland and stated that s/he never received Metformin Tab 1000 mg ER from Heartland.

However, between September 2014 and February 2018, Heartland billed S.H.'s Medicare insurance for Metformin Tab 1000 mg ER approximately 15 times. Metformin Tab 1000 mg ER is one of the top shortage medications that Qlarant identified. S.H. surmised that Ghussin billed his/her Medicare insurance for Metformin Tab 1000 mg ER, but dispensed Metformin Tab 500 mg ER.

45. As a second example, S.H. stated that s/he never received Chantix from Heartland because s/he was afraid to take Chantix due to already taking anti-depressants. However, between October 2016 and May 2017, Heartland billed S.H.'s Medicare insurance for Chantix approximately eight times.

Heartland 2

Qlarant Invoice Reconciliation

46. An FBI agent and I requested drug purchase records and received responses from the pharmaceutical wholesalers used by Heartland 2, which are listed below. An FBI agent and I furnished all of the wholesaler records and Medicare and Medicaid data received to Qlarant and requested an invoice review for the period of December 15, 2012 through June 4, 2019. Qlarant compared invoices for Heartland 2's drug purchases to Medicare and Medicaid claims data for this period.

47. On November 22, 2019, Qlarant provided the following summary of its invoice review:

> **Wholesalers with Supportive Invoices:** Alpine, Anda, Bonita, Cardinal/Harvard Drug, Fagron, Health Source, Ixthus, Keysource/ Praxis,

Masters, McKesson, Miami Luken, Parmed/ Gensource, Pharmsource, Redmond and Greer, Republic, River City, Smith Drug and Integral, South Point, Taiga, and Wasatch.

Date Range of Invoice Review: 12/15/2012 – 06/04/2019

Number of Drugs Reviewed: 101

Total Number of Drugs Short to Medicare: 43

Total Number of Drugs Short to Medicaid: 4

Approximate Loss to Medicare: $378,885.27

Approximate Loss to Medicaid: $16,098.20

Approximate Combined Loss to Medicare and Medicaid: $394,983.47

48. Qlarant provided the following summary of Heartland 2's top ten drug shortages by approximate combined loss to Medicare and Medicaid:

Drug Name	Approx. Dollar Loss
Betaseron Inj 0.3 MG	$78,781.42
Opana ER Tab 40 MG	$30,506.21
Creon Cap 24000 UNT	$26,711.94
Spiriva Cap Handihlr	$24,019.15
Latuda Tab 40 MG	$23,005.97
Latuda Tab 20 MG	$21,226.51
Latuda Tab 120 MG	$18,745.35
Lantus Solos Inj 100/ML	$16,544.91
Lidocaine Pad 5%	$16,489.45
Advair Disku Aer 250/50	$14,624.75

49. In sum, Qlarant concluded that Heartland 2's inventory of prescription drugs was not sufficient to support its claim submissions to Medicare and Medicaid for at least 43 of the 101 drugs selected for the analysis. Based upon the shortage detected,

Qlarant concluded that Medicare and Medicaid paid Heartland 2 approximately $394,983.47 for medications that Heartland 2 did not have sufficient inventory to dispense. The shortage drugs that caused the highest dollar loss were Betaseron Inj 0.3 MG, Opana ER Tab 40 MG, and Creon Cap 24000 UNT.

Beneficiary Interview

50. In December 2019, An FBI agent and I interviewed C.M., a Medicare beneficiary who picked up prescriptions at Heartland 2. Claims data reflects prescriptions purportedly dispensed to C.M. from at least 2013 to 2018. C.M. identified Ghussin as the pharmacist at Heartland and as a fill in pharmacist at Heartland 2. C.M. stated that s/he did not receive all of the medication that Heartland 2 billed to his/her Medicare insurance.

51. For example, C.M. recalled that s/he received inhalers from Heartland 2, but only received one brand of inhaler in a given month. C.M. did not receive a Proair inhaler and a Dulera inhaler in the same month. However, C.M. was billed for both a Dulera inhaler and a Proair inhaler in March 2014, May 2014, June 2014, and July 2014.

PROBABLE CAUSE: SUBJECT TELEPHONE

52. Based on my training and experience, pharmacy owners, especially when multiple people own a pharmacy, use their cellular phones to conduct pharmacy business, whether by phone call, text message, email, messaging apps, or other apps.

In addition, in my experience, conspirators in illegal fraud schemes utilize cellular telephones to communicate about the scheme. Further, based on my training and experience, I know that cellular phones can contain years of information, including information carried over from previous devices. This is particularly true with Apple cellular phones.

53. On February 10 and 12, 2020 FBI and HHS-OIG agents in Michigan interviewed former Heartland and Heartland 2 Pharmacy employee, K.S. K.S. provided the following information: K.S. worked at Heartland and Heartland 2 from October 2018 until around the time they closed (June 2019). Ghussin told K.S. he had partners from Michigan for both Heartland and Heartland 2. Ghussin told K.S. his partners were causing him stress and that he could not make decisions without them. Ghussin spoke constantly about how he had to speak with his Michigan partners to make decisions regarding the pharmacies. Ghussin had long conversations on his phone about business and he was always texting. K.S. identified Ghussin's phone number as (937) 829-1012. The toll records for Ghussin's cellular phone number reflected 662 contacts with K.S.'s phone between October 10, 2018 and January 28, 2020.

54. An FBI agent and I received wireless subscriber and toll records for the Subject Telephone pursuant to a Grand Jury subpoena served on AT&T. A review of the subpoenaed AT&T records revealed the following: AT&T phone number

(937) 829-1012 was assigned to IMEI number 353807084250860. The subscriber information for this cellular telephone number identified the financially liable party, billing party, and user information as Hartland [sic] Pharmacy, 3000 Far Hills Ave., Dayton, OH 45429. These records also indicated Hartland [sic] had been a customer since December 23, 2016.

55. Agents obtained cellular telephone numbers for Abdallah, Hamaed, and Singh through reviewing records from cellular telephone providers, Medicare, Medicaid, and PBM documentation, and public records. AT&T provided toll records for the telephone number (937) 829-1012 for the period January 1, 2012 to February 6, 2020. Ghussin's cellular phone had 8,378 contacts with Abdallah's cellular phone number between January 7, 2012 and November 26, 2019; 1,216 contacts with Hamaed's cellular phone numbers between January 6, 2012 and June 4, 2019; and 1,105 contacts with Singh's cellular phone number between February 20, 2012 and December 16, 2019. Ghussin's cellular phone had 248 contacts with Heartland between September 28, 2012 and September 10, 2019 and 85 contacts with Heartland 2 between November 26, 2012 and May 2, 2019.

56. FBI and HHS-OIG agents in Michigan received records from the Ohio Board of Pharmacy. The records included a September 1, 2017 email that Ghussin sent to a State of Ohio employee. The subject of the email was "Steve Hammond." According to Ohio unemployment insurance records, Hammond was a Heartland

employee during this time. The email concerned an Ohio Board of Pharmacy inspection finding that one of Ghussin's employees did not have a proper background check completed as required by regulation. The email address used by Ghussin was drghussin@yahoo.com. The bottom of the email had the words, "Sent from my iPhone.

57. Based on this information and my experience investigating fraudulent home health schemes, there does exist, and I do believe there exists, probable cause that Ghussin is using the Subject Telephone in furtherance of the conspiracy and that evidence or fruits or instrumentalities of unlawful conduct, including data, emails, voicemails and text messages, will be found on the Subject Telephone.

TECHNICAL TERMS

58. Based on my training and experience, I use the following technical terms to convey the following meanings:

- Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to

enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play

audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that

antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
- IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that

computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

59. Based on my training, experience, and research, I know that the Subject Telephone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

60. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

61. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Telephone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Telephone because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

62. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

UNLOCKING DEVICE WITH BIOMETRIC FEATURES

63. The records obtained from AT&T have identified the device that is tied to phone number (937) 829-1012, and IMEI number: 353807084250860 is an Apple iPhone 7 Plus.

64. 94. The warrant I am applying for would permit law enforcement to compel Ghussin to unlock the Subject Telephone using biometrics. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front

of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises.

Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, this warrant seeks authorization to search the Subject Telephone. The passcode or password that would unlock the Subject Telephone is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Subject Telephone, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some

circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID (1) when more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

65. Due to the foregoing, if the Subject Telephone may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe Ghussin's fingers (including

thumbs) to the fingerprint scanner of the Subject Telephone; (2) hold the Subject Telephone in front of Ghussin's face and activate the facial recognition feature; and/or (3) hold the Subject Telephone in front of Ghussin's face and activate the iris recognition feature, for the purpose of attempting to unlock the Subject Telephone in order to search the contents as authorized by this warrant.

SPECIAL INSTRUCTION REGARDING REVIEW OF THE SEIZED MATERIAL

66. With respect to law enforcement's review of the seized material identified in Attachment B, law enforcement (*i.e.*, the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the seized material (collectively, the "Review Team") are hereby authorized to review, in the first instance, the seized material.

67. If, during the review of the seized material, the review team finds potentially privileged materials, the Review Team will: (1) immediately cease its review of the potentially privileged materials at issue; (2) segregate the potentially privileged materials at issue; and (3) take appropriate steps to safeguard the potentially privileged materials at issue.

68. Nothing in this Instruction shall be construed to require the Review Team to cease or suspend review of all the seized material upon discovery of the existence of potentially privileged materials within a portion of the seized material.

CONCLUSION

69. Based on the foregoing, there is probable cause to believe, and I do believe, that the Subject Telephone will contain the items set forth in Attachment B, which constitute evidence, fruits of crime, contraband, and/or instrumentalities of the violations of Title 18, United States Code, Section 1347 (Health Care Fraud), Title 18, United States Code, Section 1343 (Wire Fraud), Title 18, United States Code, Section 1349 (Conspiracy to Commit Health Care Fraud and Wire Fraud), and Title 21, United States Code, Section 841 (Unlawful Distribution of a Controlled Substance).

REQUEST FOR SEALING

70. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Michael Pemberton, Special Agent
HHS-OIG

Sworn to before me and signed in my presence and/or by reliable electronic means.

Hon. Sharon L. Ovington
United States Magistrate Judge

Dated: 03/14/20

ATTACHMENT A

A cellular telephone with phone number (937) 829-1012 and IMEI number: 353807084250860 ("Subject Telephone") or any phone assigned that phone number in the event that the number has been or was re-assigned to a different phone.

ATTACHMENT B – ITEMS TO BE SEIZED

Particular Things to Be Seized

All records and information on the Subject Telephone described in Attachment A that constitute fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1347, Health Care Fraud; Title 18, United States Code, Section 1343, Wire Fraud; Title 18, United States Code, Section 1349, Conspiracy to Commit Health Care Fraud and Wire Fraud, and Title 21, United States Code, Section 841 (Unlawful Distribution of a Controlled Substance), including but not limited to:

1. Content of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, voicemails, social media account activity (including browser history, web page logs, and search terms entered by the user), photos, WhatsApp content and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above;

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of the times the devices were used;

4. Passwords, encryption keys, and other access devices that may be necessary to access the devices;

5. Contextual information necessary to understand the evidence described in this

attachment, all of which constitute evidence, fruits and instrumentalities of the violation described above.

6. During the execution of the search of the property described in Attachment A, law enforcement personnel are authorized to (1) press or swipe Kindy Ghussin's ("Ghussin") fingers (including thumbs) to the fingerprint scanner of the Subject Telephone; (2) hold the Subject Telephone in front of Ghussin's face and activate the facial recognition feature; and/or (3) hold the Subject Telephone in front of Ghussin's face and activate the iris recognition feature, for the purpose of attempting to unlock the Subject Telephone in order to search the contents as authorized by this warrant.